Docket No. 010034   Serial No. 09/828,556

REMARKS/ARGUMENTS

Claim 1-20 are pending in the present application.

The Applicant filed the original application on April 5, 2001. The Examiner mailed the first, non-final Office Action on September 24, 2004. A Response to that Office Action was filed. The Examiner mailed a second, non-final Office Action on March 24, 2005. A Response to that Office Action was filed. The Examiner mailed a third, non-final Office Action on September 8, 2005. The remarks herein are in response to the third Office Action.

Objection to the Specification

The Examiner objected to the disclosure because it contains embedded hyperlinks and/or other form of browser-executable code. MPEP 608.01 objects to hyperlinks beginning with http// and followed by a URL address, but does not object to URL addresses alone. Therefore, the Applicant amends the specification to change hyperlinks to URL addresses to overcome the Examiner's objection.

Rejection under 35 U.S.C. 103(a)

Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boneh, et al (Pub. No. 2002/0112167) (Boneh) in view of Jones, et al. (U.S. Patent No. 6,088,800) (Jones).

As succinctly stated in the MPEP, to establish a prima facie case of obviousness, three basic criteria must be satisfied:

"First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine the teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claimed limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on the applicant's disclosure." Section 706.02(j) (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

3

Docket No. 010034   **Serial No. 09/828,556**

"To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." MPEP 706.02(j) (quoting *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)).

The Applicant respectfully traverses the rejection.

The Applicant submits that the combination of Boneh and Jones does not teach or suggest all the claimed limitations in any of the independent claims.

<u>Teachings of Boneh:</u>

Boneh teaches, in the Abstract: "A method and apparatus are provided for *protecting sensitive information within server* or other computing environments. Numerous electronic requests addressed to a server system are received over network couplings and evaluated. The evaluation scans for sensitive information including credit card information and private user information. Upon detecting sensitive data, *cryptographic operations are applied to the sensitive data.* When the sensitive data is being *transferred to the server system,* the *cryptographic operations encrypt the sensitive data prior to transfer* among components of the server system. When sensitive data is being *transferred from the server system,* the *cryptographic operations decrypt the sensitive data prior to transfer* among the network couplings. The cryptographic operations also include hash, and keyed hash operations." (emphasis added)

Boneh teaches that one or more TE Appliances (e.g., 102, 202, 204) perform the encryption and/or decryption.

Boneh teaches that function of the TE Appliances may be dedicated network appliances or distributed among various associated network components (page 2, par. 0027)

Boneh teaches: "When the TE Appliance identifies tags indicating that the associated data is sensitive, it applies an *appropriate cryptographic operation* to the data within these tags, in block 306. For example, incoming sensitive data is *encrypted using known encryption algorithms* such as know public key infrastructure ("PKI") encryption algorithms or the Data Encryption Standard ("DES")." (page 2, par. 29) (emphasis added)

4

Docket No. 010034   **Serial No. 09/828,556**

Boneh, at page 5, par. 0061 and 0062, as cited by the Examiner, merely provides a general description of a "processor," including CPUs, DSPs, and ASICs, and a general description of a "computer-readable media," respectively.

Teachings of Jones:

Jones teaches three *known encryption algorithms*, including DES and RC5 (both standard IPSEC algorithms), and IDEA (i.e., a PGP encryption algorithm). (col. 5, lines 49-53)

The Applicant also incorporates by reference, but excludes for the sake of brevity herein, the Applicant's extensive analysis of Jones in the Applicant's previous response dated June 24, 2005 in reply to the Examiner's previous Office Action dated March 24, 2005.

Applicant's remarks on Boneh and Jones:

The Examiner's citation of Jones adds little new to a combination with Boneh because Jones example of a DES encryption algorithm (col. 5, lines 49-53) is also taught in Boneh (page 2, par. 29).

As to independent claim 1, Boneh, alone or in combination with Jones, does not teach or suggest at least the following underlined portions.

1. A device for <u>accelerating functioning of a software application</u> having multi-layer, high overhead protocols, the device comprising:

a first processor operating a software application having a multi-layer protocol;

<u>a high performance processor configured to operate one layer of the multi-layer protocol according to a command from the first processor;</u> and

<u>a memory accessible to each of the first processor and the high performance processor for passing commands and data between the first processor and the high performance processor.</u>

5

As to independent claim 7, Boneh, alone or in combination with Jones, does not teach or suggest at least the following underlined portions.

7. A device for <u>accelerating security protocols</u>, the device comprising:

a multi-layer security protocol having one or more of an encryption algorithm and <u>an authentication algorithm</u>;

<u>a shared memory</u>;

<u>a processor coupled to the memory and operating a first portion of a predetermined one of the security protocols</u>; and

<u>a high performance processor coupled to the memory and operating a second portion of the predetermined one of the security protocols</u>.

As to independent claim 12, Boneh, alone or in combination with Jones, does not teach or suggest at least the following underlined portions.

12. A circuit for <u>partitioning a multi-layer security services protocol</u>, the circuit comprising:

<u>a shared memory</u>;

<u>first and second processor cores coupled to the shared memory</u>;

a multi-layer security services protocol <u>partitioned between each of the first and second processor cores</u>;

<u>one or more application program interfaces operated by the first processor core for interfacing between the security services protocol and the second processor core; and</u>

<u>a modular math function operating on the second processor core</u>.

As to independent claim 15, Boneh, alone or in combination with Jones, does not teach or suggest at least the following underlined portions.

15. A method for <u>accelerating a multi-layer protocol</u>, the method comprising:

<u>partitioning a function of a multi-layer protocol in a first processor</u>;

<u>distributing the function to a second high performance processor via a memory shared by both the first and second processors</u>;

<u>performing the distributed function in the high performance processor</u>; and

<u>returning a result of the distributed function from the high performance processor via the shared memory</u>.

6

Docket No. 010034   Serial No. 09/828,556

In summary, Boneh, alone or in combination with Jones, appears to teach or suggest applying an *"appropriate cryptographic operation,"* using *"known encryption algorithms* such as know public key infrastructure ("PKI") encryption algorithms or the Data Encryption Standard ("DES")." (page 2, par. 29) Boneh's description of a "processor" and a "computer-readable media," at page 5, par. 0061 and 0062, respectively, merely generally describes these terms.

"The present invention provides a device and method that helps to accelerate the complex encryption and authentication algorithms exist within the security protocols by partitioning the cryptographic layers and distributing them to a high performance processor, such as a digital signal processor. The present invention thereby provides a high performance computing engine that implement the functions within these algorithms with a minimum of delay and a minimum cost to the consumer." (Summary of the Invention, par. 1)

Therefore, the present invention is an improvement over the known encryption algorithms, as taught by Boneh, alone or in combination with Jones.

The present application was filed on April 5, 2001, and the oath or declaration for the present application was signed on March 21, 2001. Boneh has a provisional filing date of January 4, 2001. 35 U.S.C. 102(e) states: "the invention was described in — (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent." If necessary, the Applicant reserves the right to overcome the present rejection under 35 U.S.C. 103(a) also by showing that Boneh's provisional filing date of January 4, 2001 is after the invention by the applicant for patent.

In view of the foregoing, Applicant submits that all pending claims are in condition for allowance. Applicant respectfully requests the reconsideration and reexamination of this application and the timely allowance of the pending claims. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

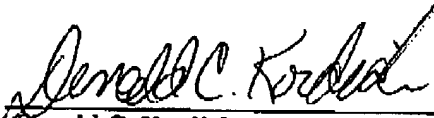**Docket No. 010034**   **Serial No. 09/828,556**

If there are any other fees due in connection with the filing of the response, please charge the fees to our Deposit Account No. 17-0026. If a fee is required for an extension of time under 37 CFR 1.136 not accounted for above, such an extension is requested and the fee should also be charged to our Deposit Account.

Applicants therefore respectfully request that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

Dated: _____March 8, 2006_____   By: _____
                                                  Donald C. Kordich
                                                  Attorney for Applicant
                                                  Registration No. 38,213

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121-2779
Telephone: (858) 658-5928
Facsimile: (858) 658-2502

8